Call Appearance: Means an instance of a call or call attempt with direct subject control, as defined in J-STD-025. For example, a party with three call appearances may be involved in and control three calls simultaneously. Some services that do not permit the subject to directly control the call, such as call forwarding, do not consume [use up] call appearances.

Call Content: Means, when used with respect to any wire or electronic communication, any information concerning the substance, purport, or meaning of that communication, as defined in 18 U.S.C. § 2510(8), and includes any transfer of messages, signals, writing, images, sounds, data, or intelligence of any kind by or to a subject.

Call Content Channel (CCC): Means the logical link between the device performing an electronic surveillance access function and the law enforcement agency that primarily carries the call content passed between a subject and one or more associates, as defined in J-STD-025.

Call Data Channel (CDC): Means the logical link between the device performing an electronic surveillance access function and the law enforcement agency's collection equipment that primarily carries call-identifying information, as defined in J-STD-025.

Call Forwarding: Means any of the several features that redirect a call to another directory number (or voice mail) if a certain condition (or set of conditions is met), as defined in J-STD-025.

Call-Identifying Information: Means all dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subject by means of any equipment, facility, or service of a telecommunications carrier, as defined in CALEA Section 102(2), 47 U.S.C. § 1001(2).

Call Leg: Means a bi-directional call path associated with each network facility usage attempt and subsequent usage, as defined in J-STD-025.

Circuit: Means a switchable bi-directional path between two locations, as defined in J-STD-025. A circuit may be all or part of a channel. On an end-to-end circuit, separate physical facilities may be used for each segment of the circuit.

Circuit-Mode: Means a communication using bi-directional paths switched or connected when the communication is established. The entire communication uses the same path.

Communication: Means any wire or electronic communication, as defined in 18 U.S.C. § 2510.

Complete: Means a call attempt that is answered.

Connection: Means a relationship between two or more parties of a call to allow communication between them.

Cut-Through: Means the completion of a connection in one direction (partial), or both directions (full), between two call appearances.

Demarcation Point: Means the point separating the telecommunications carrier's facilities from government-procured delivery facilities and is the point at which a telecommunications carrier transfers the intercepted call content and call-identifying information to the law enforcement agency.

Intercept Access Point (IAP): Means the point at which a telecommunications carrier accesses communications or call-identifying information.

Interface: Means the format defining the information to be exchanged, and the procedures for generating, sending, receiving, and processing that information, that must be selected and used by both parties in order for communications to take place between a telecommunications carrier's network and a law enforcement agency's equipment. The Open Systems Interconnection (OSI) Reference Model of the International Telecommunications Union (ITU) provides a common language describing the sequence of hardware or software protocols (i.e., the protocol stack) that must be used by the Interface to enable communication.

Subject: Means a person who uses telecommunications equipment, facilities, or services that are subject to a court order or other lawful surveillance authorization, and whose communications or call-identifying information are intercepted and delivered to a law enforcement agency.

Subscriber: Means the person or entity whose telecommunications equipment, facilities, or services are subject to a court order or other lawful surveillance authorization providing that the communications or call identifying information, or both, carried by that equipment, or supported by those facilities or services, are to be intercepted and delivered to a law enforcement agency.[2]

---

[2] The term "Intercept Subject" is defined in J-STD-025 as the "telecommunications service subscriber whose communications, call identifying information, or both, have been authorized by a court to be intercepted and delivered" to a law enforcement agency. As a legal matter, however, a court order or other lawful surveillance authorization under 18 U.S.C. §§ 2510-2522 (content), or 18 U.S.C. §§ 3121-27 (call-identifying information), applies to the telecommunications equipment, facilities, or services under surveillance, not to the communications of a specific individual. 18 U.S.C. § 2518(4)(b); *id.* § 2518(1)(B)(ii); *id.* § 3123(b)(1)(C). Section 64.1708 of this Part therefore does not adopt the "Intercept Subject" nomenclature used in J-STD-025. The term "Subscriber" is used in Section 64.1708 to identify the person whose telecommunications equipment, facilities, or services are under surveillance. The term "Subject" is used to identify the parties whose communications and call-identifying information are intercepted and delivered to a law enforcement agency; these parties may include the Subscriber (as that term is defined herein), or other persons who use the Subscriber's telecommunications equipment, facilities, and services.

Telecommunications Carrier: Means "telecommunications carrier," as that term is defined in CALEA Section 102(8), 47 U.S.C. § 1001(8).[3]

4. Sections 64.1706 through 16.1708 are added, to read as follows:

§ 64.1706 *Electronic Surveillance Standards.* Telecommunications carriers shall comply with the assistance capability requirements set forth in Section 103 of CALEA, 47 U.S.C. §1002. In order to comply with these assistance capability requirements, telecommunications carriers shall ensure that their equipment, facilities, or services that provide a customer with the ability to originate, terminate, or direct communications provide the electronic surveillance assistance capabilities defined in the electronic surveillance interface standards set forth in Sections 64.1707 through 64.1708, below.

§ 64.1707 *Interim Standard J-STD-025 Assistance Capabilities.* Telecommunications carriers shall ensure that their equipment, facilities, or services that provide a customer with the ability to originate, terminate, or direct communications provide the electronic surveillance assistance capabilities defined in the electronic surveillance interface standards set forth in Interim Standard J-STD-025, TIA/EIA/IS-J-STD-025, (December 1997), published jointly by the Telecommunications Industry Association (TIA) and the Alliance for Telecommunications Industry Solutions (ATIS). This incorporation by reference was approved by the Director of the Federal Register in accordance with 5 U.S.C. § 552(a) and 1 CFR part 51. Copies of the document may be inspected at the Federal Communications Commission, 1919 M Street, NW., Washington, DC 20554 or at the Office of the Federal Register, 800 N. Capitol Street, NW., Washington, DC. Copies of J-STD-025 can be obtained from the Commission's contract copier or from Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5704 (1-800-854-7179) or the Alliance for Telecommunications Industry Solutions, 1200 G Street, N.W., Suite 500, Washington, DC 20005 (202-628-6380).

§ 64.1708 *Additional Assistance Capabilities.* In addition to the assistance capabilities defined in J-STD-025 and referenced in Section 64.1707, above, telecommunications carriers shall ensure that their equipment, facilities, or services that provide a customer with the ability to originate, terminate, or direct communications provide the following additional electronic surveillance assistance capabilities:

(a) *All Content of Conferenced Calls.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of providing to law enforcement all content of conferenced calls over a subscriber's equipment, facility, or services, where capability is defined as the ability to monitor a multiparty or conference call established by the subscriber's equipment,

---

[3] The Federal Communications Commission is also addressing the definition of "telecommunications carrier" in the pending rulemaking proceeding *In the Matter of the Communications Assistance for law Enforcement Act,* CC Docket No. 97-213 (released October 10, 1997).

features, or services where two or more parties are allowed to converse after the subject leaves the conversation, temporarily or permanently.

(a)(1) For subject-initiated multiparty calls, multiple CCCs may be necessary if the subscriber's service will support communications with two or more associates. CCCs shall follow the subscriber's terminal. A separate CCC shall monitor the subscriber's conference service when the subject is separated from the subject's conference. Call content shall be delivered to law enforcement whenever the subscriber's service continues to support the communications of the associates.

(a)(2) On a subject-initiated multiparty call, call content shall not be delivered over the CCC when the subject leaves the multiparty call and only one party remains on the multiparty call.

(b) *Party Hold, Party Join, and Party Drop Messages.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of providing messages to law enforcement that enable law enforcement to identify the parties to a conversation at all times.

(b)(1) *PartyDrop.* The PartyDrop message reports when one or more parties to a call are released and the call continues with two or more other parties. The PartyDrop message shall be triggered and delivered when a party is released from a multi-way call (e.g., three-way calling, conference call, meet-me conference). The PartyDrop message shall not be triggered when an entire call is released, which is reported by the Release message.

(b)(2) The PartyDrop message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 1: PartyDrop Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber.
IAPSystemIdentity	C	Identifies the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.

CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
One of Released Party Identities Remaining Party Identities	M	 Identifies parties released from the call. Identifies parties remaining in the call.

(b)(3) The PartyDrop message shall adhere to the following ASN.1 syntax definition:

```
PartyDrop :: = SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity     OPTIONAL,
        -- Include to identify the system containing the IAP when the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
        [3]     CallIdentity,
    CHOICE {
releasedParties         [4]     SEQUENCE OF PartyIdentity,
remainingParties    [5]     SEQUENCE OF PartyIdentity}}
```

(b)(4) *PartyHold.* The PartyHold message reports the placing of one or more parties of a call on hold by the subject. The PartyHold message shall be triggered and delivered when one or more parties are no longer connected to a call through use of one of the following features: (i) call hold; (ii) call waiting; (iii) three-way calling; (iv) conference call or meet-me conference; and (v) other similar features or services.

(b)(5) The PartyHold message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 2: PartyHold Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber.
IAPSystemIdentity	C	Identifies the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.

CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
One of Held Party Identities Remaining Party Identities	M	 Identifies parties placed on hold. Identifies parties remaining in the call.

(b)(6) The PartyHold message shall adhere to the following ASN.1 syntax definition:

```
PartyHold :: = SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity    OPTIONAL,
        -- Include to identify the system containing the IAP when the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
        [3]     CallIdentity,
    CHOICE {
heldParties     [4]     SEQUENCE OF PartyIdentity,
remainingParties [5]    SEQUENCE OF PartyIdentity}}
```

(b)(7) *PartyJoin.* The PartyJoin message reports the addition of a call party to an active call or the retrieval of a held call by the subject. The PartyJoin message shall be triggered and delivered when (i) one or more previously held associates are added to the current call (e.g., call waiting, three-way calling, conference calling) and (ii) an associate joins an existing call with a subject (e.g., barge-in).

(b)(8) The PartyJoin message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 3: PartyJoin Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber.
IAPSystemIdentity	C	Identifies the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.

CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
Joined Party Identities	M	Identifies parties that joined the call.

(b)(9) The PartyJoin message shall adhere to the following ASN.1 syntax definition:

```
PartyJoin :: = SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity              OPTIONAL,
        -- Include to identify the system containing the IAP when the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
        [3]     CallIdentity,
joinedParties   [4]     SEQUENCE OF PartyIdentity}
```

(c) *Subject-Initiated Dialing and Signaling.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of providing law enforcement with access to all subject-initiated dialing and signaling, including the use by a subject of flash hooks, feature keys, and all other key usage.

(c)(1) For all subject-initiated dialing and signaling, a message shall be triggered and delivered, which message may be the origination message, that reports subject inputs of flash hooks and other key usage signaled to the network through the use of the following triggers: (i) when a switchhook flash or its equivalent is detected and (ii) when a key press signaled to the network is detected.

(c)(2) The nature of number and presentation/restriction indicators parameters signaled with a telephone number shall be reported in the Context [18] sub-parameter of the PartyIdentity parameter, as defined in J-STD-025.[4]

(c)(3) Origination messages as defined in J-STD-025 shall also be triggered and delivered when the subject goes off-hook without dialing (with

[4] The nature of number and presentation/restriction indicators parameters signaled with a telephone number are referred to in the discussion of party identity features contained in ITU-T *Number Identification Services,* ITU-T I.251, at §§ 251.3 (Calling Line Identification Presentation) and 251.4 (Calling Line Identification Restriction).

a corresponding Release message sent when the subject goes back on-hook).

(d) *Notification Messages for In-band and Out-of-band Signaling.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of providing notification messages to law enforcement over the CDC of in-band and out-of-band signaling from the subscriber's service throughout each call. Notification messages shall be triggered and delivered to the law enforcement agency to report out-of-band signaling delivered through a subscriber's service that can be sensed by the subject and to report in-band signaling applied by the equipment, facilities, or services supporting the subscriber's terminal.

(d)(1) The Notification message shall be triggered and delivered when the accessing system applies an in-band audible indication to the subscriber's receive content channel or sends or passes a command to the subscriber's terminal to activate, deactivate, or control generation of the following indications of incoming calls or messages:

(A) any alerting of incoming calls or messages;

(B) audible indications of incoming calls or messages (e.g., call waiting tone, message waiting tone, power alert/ring, distinctive alert/ring, recall alert/dial tone, call forwarding reminder alert/ring, busy tone, or reorder tone);

(C) visual indications of incoming calls or messages (e.g., lights to indicate call waiting); and

(D) alphanumeric display information (e.g., messages sent to the terminal, calling number identification, or calling name identification).

(d)(2) The Notification message for in-band and out-of-band signaling shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 4: Notification Message Parameters

Parameter	MOC	Usage

CaseIdentity	M	Identifies the Subscriber.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
Audible Visual or Displayed Signal	M	Identifies the audio signal, visual signal, or displayed text sensed by the Subscriber or Subject.

(d)(3) The Notification message for in-band and out-of-band signaling shall adhere to the following ASN.1 syntax definition:

```
Notification :: = SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity    OPTIONAL,
        -- Include to identify the system containing the IAP when the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
        [3]     CallIdentity,
audioVisualDisplay  [4]     VisibleString (SIZE (1..128) )}
```

(e) *Timely Delivery of Call-Identifying Information.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of expeditiously accessing and delivering call-identifying information to law enforcement contemporaneously with the communications to which it pertains, or in a manner comparable to the speed with which other signaling messages are sent in the public network so that call-identifying information may be associated with the related communications. The following requirements shall apply to the delivery of call-identifying information.

(e)(1) Each CDC message shall contain a time stamp required to associate and synchronize the message to the call content delivered separately over a CCC. The time stamps shall be generated using the clock of the network element containing the IAP. The time stamp on each of the call event messages shall be accurate within 100 milliseconds (ms) of the triggering events described in J-STD-025 for each message.

(e)(2) The activation of a CCC shall contain an event that marks a change from an idle state to an active state (e.g., the transmission of the time stamp and serial number) that is detectable at the collection function. The CCOpen message time stamp shall mark (within 100 ms) the

change in status and shall be the timing reference for correlation of CDC message times to the CCC call content flow.

(e)(3) To enable law enforcement to correlate CDC messages with CCC information, call event messages shall be delivered from the IAP to the demarcation point at the carrier facility in as near real time as possible, but no later than three seconds after the occurrence of the associated call event, with a probability of 99%.

(e)(4) The delivery timing requirements shall be measured from when the reported event occurs at the IAP until the first bit of each event message begins transmission on the government procured facilities.

(e)(5) The following messages shall be delivered to the demarcation point within no more than 5 seconds (99% probability): (i) Serving System Message; (ii) Feature Status Message; and (iii) Surveillance Status Message.

(e)(6) To ensure that their equipment, facilities, or services are capable of providing information that enables law enforcement to correlate a set of call-identifying information messages from the CDC to a segment of call content received on a CCC, telecommunications carriers shall transmit a unique tag both in-band on the CCC and over the CDC in the CCOpen message.[5] Signaling on the CCC shall be used to inform law enforcement when call content is being delivered and to provide an event on the CCC with which the CCOpen message time stamp can be associated.

(A) The values of the CCOpen message TimeStamp parameter followed by the CCCSerialNumber parameter shall be transmitted using industry standard in-band signaling (i.e., DTMF, MF, or FSK) on the CCC immediately before call content delivery.[6]

---

[5] Although any set of messages from one call may share a common call identity, call identities will be reused frequently. In addition, several calls may be received sequentially over the same CCC within a short time period. Because network and collection equipment clocks are not synchronized and may differ by minutes or hours, an additional measure is needed for correlation.

[6] The time between call origination and answer generally allows sufficient time to transmit such a tag without overriding any portion of the call content.

(B) The time stamp of the CCOpen message shall coincide with the start of delivery on the CCC. The CCCSerialNumber, appended to the CCOpen-message TimeStamp, shall be transmitted in-band on the CCC immediately prior to transmission of call content and enables that content to be directly associated with that CCOpen message.

(C) The CCOpen message as defined in J-STD-025, shall be modified to include the following parameter:

Table 5: CCC Serial Number Parameter (Addition to J-STD-025, Table 3)

CCC Serial Number	M	Uniquely correlates CDC messages to a particular call content transmitted on the CCC.

(D) The CCOpen message initially shall be used to associate a particular call with a CCC on the dedicated circuit. If that call is later merged into another call and supported by another CCC, a Change message shall be delivered to maintain the association between the communication and the channel(s) on which it is delivered.

(E) A serial number parameter shall be added to the CCOpen containing the following ASN.1 syntax definition:

```
CCOpen ::= SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity    OPTIONAL,
        -- Include to identify the system containing the IAP when the
        -- underlying data carriage does not imply that system.
        [2]     TimeStamp,
CHOICE {[3]     SEQUENCE OF CallIdentity, -- for circuit-mode intercepts
        [4]     PDUType,  -- for packet-mode intercepts},
        [5]     EXPLICIT CCCIdentity,
        [6]     CCCSerialNumber -- for correlation of CDC to CCC}
```

(F) The CCCSerialNumber parameter shall be a number that is assigned sequentially on a per CCC basis and shall not repeat within a 24-hour period. The CCCSerialNumber shall always be greater than zero, and shall be reset each day at midnight using local time.

```
CCCSerialNumber ::= VisibleString (SIZE (1..4) )
```

(f) *Surveillance Status Message.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of delivering a Surveillance Status message confirming that the interception software is working correctly and accessing the equipment, facilities, or services of the correct subscriber. The receipt of the Surveillance Status message over the CDC verifies that the CDC is operational.

(f)(1) The SurveillanceStatus message shall be triggered and delivered whenever a surveillance is activated, updated, or deactivated.

(f)(2) The SurveillanceStatus message shall also be sent periodically from once every hour to once every 24 hours for the duration of a surveillance. Updates concern changes to the number and identity of CCCs provisioned for the particular CaseIdentity.

(f)(3) The activate and update SurveillanceStatus messages shall report any call content channels assigned to the surveillance.

(f)(4) The SurveillanceStatus message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 6: SurveillanceStatus Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
SurveillanceStatusType	M	Identifies the type of SurveillanceStatus report.
Provisioned CCCs	C	Included when call content channels are provisioned.

(f)(5) The SurveillanceStatus message shall adhere to the following ASN.1 syntax definition:

```
SurveillanceStatus :: = SEQUENCE {
        [0]    CaseIdentity,
        [1]    IAPSystemIdentity                    OPTIONAL,
```

```
                    -- Include to identify the system containing the IAP when the
                    -- underlying data carriage does not imply that system.
                    [2]     TimeStamp,
                    [3]     SurveillanceStatusType,
provisionedCCCs     [4]     SEQUENCE OF EXPLICIT CCCIdentity    OPTIONAL}
```

(f)(6) The SurveillanceStatus message shall include a SurveillanceStatusType parameter indicating the type of status reported in the following manner:

```
SurveillanceStatusType ::= ENUMERATED {
                               activated     (0),
                               updated       (1),
                               inProgress    (2),
                               deactivated   (3)}
```

(g) *Feature Status Message*. Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of delivering a Feature Status message that reports when a request is made by a subscriber, subject, or the service provider for the assignment, removal, activation, or deactivation of network-provided features, even when the subscriber, or a subject, modifies capabilities remotely through another phone or an operator unaware of an interception.[7] The FeatureStatus message shall report when a subscriber first gains or loses the ability to invoke, without delay, network-provided features that would affect the delivery to law enforcement of call content or call-identifying information related to that subscriber's equipment, facilities, or services. The FeatureStatus message is not required when a new capability is gained through the subscriber's terminal and is reported by other messages.

(g)(1) The FeatureStatus message shall report features that are assigned or removed as a result of service provider actions, or that are activated or deactivated remotely by using another's equipment, facilities, or services. The Feature Status message does not need to be reported when the assignment, activation, deactivation, or removal of new features are detectable through other messages described in J-STD-025.

---

[7] *See generally* TIA/EIA/IS-41.5-C, at p. 150 [¶ 6.5.2.20] (February 1996) (description of "CallingFeatures Indicator").

(g)(2) The FeatureStatus message shall be triggered and delivered when the service provider assigns or removes and when the subject activates or deactivates the following features:

(A) Call redirection features that affect the routing of calls, including all variations of call forwarding features (e.g., call forwarding busy and call forwarding unconditional);

(B) Multiple circuit features that affect the number of CCCs required to include all variations of multiparty features (e.g., call waiting, call hold, three-way calling, conference calling);

(C) Features that affect surveillance trigger identities (e.g., number change feature); and

(D) Service suspend and service disconnect features.

(g)(3) The FeatureStatus message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 7: FeatureStatus Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
FeatureName	M	Identifies the feature or service.
FeatureModification	M	Identifies the type of successful feature change.
FeatureParties	C	Included when the feature involves association of parties to the feature.

(g)(4) The FeatureStatus message shall adhere to the following ASN.1 syntax definition:

FeatureStatus :: = SEQUENCE {

```
                [0]     CaseIdentity,
                [1]     IAPSystemIdentity                   OPTIONAL,
                -- Include to identify the system containing the IAP when the
                -- underlying data carriage does not imply that system.
                [2]     TimeStamp,
featureName     [3]     VisibleString (SIZE (1..64) ),
                [4]     FeatureModification,
featureParties  [5]     SEQUENCE OF PartyIdentity        OPTIONAL
        -- included when feature usage records other party identities}
```

(g)(5) The FeatureStatus message capability shall include a FeatureModification parameter that indicates only successful modifications to a subscriber's capabilities. The FeatureModification parameter is defined as follows:

```
FeatureModification ::= ENUMERATED {
        assignment                      (0),
        unassignment                    (1),
        activation                      (2),
        deactivation                    (3),
        changeOfAssociatedPartyIdList   (4)}
```

(h) *Continuity Check.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of delivering a continuity check in the form of an in-band signal (e.g., idle signal as defined in ANSI T1.403, Appendix D) or tone (e.g., DTMF C-tone) that will verify that CCCs between the carrier and a law enforcement agency are in working order.

(h)(1) When dedicated circuits are used to support CCCs (nailed-up CCCs), the continuous signal or tone shall be applied to idle CCCs to verify continuity.

(h)(2) When a CCC is selected for use and opened, the signal or tone shall be removed from the channel, enabling the transmission on the CCC coincident with the generation of the CCOpen message.

(h)(3) The time stamp of the CCClose message shall coincide with the release of the CCC. This coincidence shall be indicated by the re-application of a continuous signal or tone on the CCC.

(i) *Dialed Digit Extraction.* Telecommunications carriers shall ensure that their equipment, facilities, or services are capable of extracting the digits dialed by

the subject following cut-through at the access point and delivering those digits to the law enforcement agency in a post-cut-through InBandDigits message containing the those digits.

(i)(1) The InBandDigits message shall be delivered over the CDC and shall report subject inputs detected by the accessing switch (including any DTMF tones detected) that have partially or fully cut-through a call content path from the subject toward an associate. Inputs may be accumulated for up to thirty seconds or until the maximum number of digits that can be carried by the InBandDigits message (32) is reached, whichever is earlier. Inputs accumulated in this manner shall be delivered in an InBandDigits message when an event precludes acting upon the input (e.g., call abandonment) or when the maximum number of digits that can be carried by an InBandDigits message is reached.

(i)(2) The InBandDigits message shall include the following parameters, which parameters shall be marked as either Mandatory (M), meaning required for the message, or Conditional (C), meaning required in situations where a condition (defined in the usage column of the table where it occurs) is met:

Table 8: InBandDigits Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Subscriber.
IAPSystemIdentity	C	Include to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call appearance, or call leg within a system.
UserInput	M	Identifies specific user input when it is detected.

(i)(3) The InBandDigits message shall adhere to the following ASN.1 syntax definition:

```
InBandDigits :: = SEQUENCE {
        [0]     CaseIdentity,
        [1]     IAPSystemIdentity          OPTIONAL,
        -- Include to identify the system containing the IAP when the
        -- underlying data carriage does not imply that system.
```

[2] TimeStamp,
[3] CallIdentity,
userInput [4] VisibleString (SIZE (1..32))
-- e.g., "12345" or "*123" or "#345"}

(j) *Ceiling Limit on Number of Interfaces.* The total number of Interfaces used by the telecommunications industry to implement J-STD-025, and the standards defined in sections (a) through (i) hereof, shall not exceed five Interfaces for the CDC and five Interfaces for the CCC, respectively.

(j)(1) An Interface includes a protocol sequence (i.e., the "Protocol Stack"). Each protocol layer in a Protocol Stack (i.e., the "OSI Layer") shall refer to an available industry-wide standard or widely-used protocol. An OSI Layer may be defined as a "null" layer, meaning that no protocol is used at that layer. Where appropriate (e.g., for the network layer), sub-layer protocols may be selected and identified. The following are the OSI Layers: Application, Presentation, Session, Transport, Network (Inter-network and Intra-network), Data, Link, and Physical.

(j)(2) Packet-mode CCCs may use any of the protocol stacks defined for either the CDC or CCC.

(j)(3) The following table is included for explanatory purposes:

Table 9: Interface Protocol Example

OSI Layer	**CDC Protocol Stack (d)***					**CCC Protocol Stack (b)***				
	d^1	d^2	d^3	d^4	d^5	b^1	b^2	b^3	b^4	b^5
Application										
Presentation										
Session										
Transport										
Network: Inter-network										
Intra-network										
Data Link										
Physical										

*d = data; b = bearer

Electronic Surveillance Interface Document

Issue: 1.0

June 24, 1996

Table of Contents

(This page is intentionally left blank)

1. Introduction

The Electronic Surveillance Interface (ESI) is law enforcement's recommendation for the logical and physical interfaces between a telecommunications carrier (TC) network and a law enforcement agency's (LEA) electronic surveillance collection facility. As used in this document, "electronic surveillance" refers to the interception and monitoring of communications (i.e., call content) and/or call-identifying information as set forth in a court order or other legal authorization.

Law enforcement recognizes that in many instances the telecommunications services subscribed to by certain electronic surveillance subjects may permit a TC to access and deliver the communications and call-identifying information to the LEA without the TC having to modify its networks or systems. In these instances, the TC may be fully compliant with the assistance capability requirements set forth in the Communications Assistance for Law Enforcement Act (CALEA) of 1994, Public Law 103-414. For example, a TC could effect a central office- or local loop-based interception using conventional methods of access and delivery and fully meet law enforcement's electronic surveillance needs. Increasingly, however, subjects of electronic surveillance are subscribing to advanced services and features that impede or even preclude law enforcement's full and proper execution of surveillance orders. Network-based solutions (central office-based or others) will likely be required to address these problems. This document is intended to provide guidance to TCs, in the form of law enforcement's recommendations for an electronic surveillance delivery interface, regarding electronic surveillance efforts associated with such advanced telecommunications services and features.

Although there may be a number of technical methods and interfaces for delivering intercepted communications and call-identifying information to law enforcement, the ESI recommended in this document is preferred by the law enforcement community for network-based surveillances of subjects who subscribe to advanced services and features. This ESI would satisfy law enforcement's electronic surveillance needs and would constitute an acceptable means of achieving compliance with the delivery capability requirements in Section 103 of CALEA. For TCs that adopt the ESI described herein, a series of technical requirements are set forth to support the recommended delivery interface.

This document was prepared in cooperation with representatives of the U.S. law enforcement community. Its development also involved consultations with telecommunications industry representatives, particularly technical experts from telecommunications equipment manufacturers.

1.1 Purpose and Scope

The ESI is being defined to support the implementation of CALEA. CALEA clarifies the extent to which a TC must provide capabilities to assist law enforcement in conducting lawfully authorized electronic surveillance. After the passage of CALEA, the telecommunications industry asked law enforcement to describe its vision and recommendations for the interface between a TC network and law enforcement collection equipment. This document responds to that request and serves as a technical specification for the ESI. The requirements for the ESI as defined in this document are based on law enforcement electronic surveillance needs. This

document does not address the various types of legal authorizations that dictate the specific information to be provided for a surveillance. The definition of the ESI and the subsequent deployment of network-based surveillance capabilities by TCs do not preclude LEAs from continuing to use existing, subscriber loop-based access techniques.

This document defines requirements for the delivery of both call content and call-identifying information to an LEA. It also defines the physical characteristics of the ESI and a protocol for delivering specific information elements to LEAs. It does not address any procedures for enabling access to a subject's communications nor requirements for how call-identifying information is accessed in a TC network. The document does not assume any particular network implementation or architecture for meeting the ESI requirements. However, the TCs should consult with law enforcement on alternative network implementations and architectures to ensure that the resulting access and delivery methods are cost effective for the industry and LEAs.

Definition of ESI requirements was based on analyses of widely deployed wireline and wireless services, which are described in publicly available and industry recognized standards or requirements documents. The services analyzed for this document do not encompass all services deployed in public networks today. However, the analysis of selected services provided the foundation for ESI requirements. The scope of the first issue of this document is to address law enforcement interface needs for the following telecommunications services and technologies:

- Plain Old Telephone Service (POTS)
- Centrex services
- Custom Calling features
- Custom Local Area Signaling Services (CLASS℠)
- Cellular services
- Intelligent Network (IN) services
- Advanced Intelligent Network (AIN) services
- Integrated Services Digital Network Basic Rate Interface (ISDN BRI).

Personal Communication Services (PCS) were not analyzed during the development of this version of the ESI document. However, most of the ESI requirements applicable to the cellular networks can be applied to the PCS networks. The exclusion of any particular telecommunications service or feature in the process of developing this initial ESI requirements issue should not be construed as limiting or altering the authority of LEAs to intercept call content or call-identifying information involving that service or feature, nor does it affect a TC's obligations under CALEA or other laws. Future issues of the ESI document may address other telecommunications services and technologies.

1.2 Intended Audience

TCs are responsible for meeting the assistance capability requirements set forth in CALEA, and it is incumbent on equipment manufacturers and support services providers to cooperate with TCs in meeting those obligations on a timely basis. This document is intended to offer guidance to those entities in the industry. Its use by the industry may occur under the purview of recognized industry associations and standards-setting organizations. These organizations should view the ESI document as part of law enforcement's contribution to the consultative process,